Online Safety Policy

Approved by:	The Trust Board	**Date:**	July 2023
Last reviewed in:	New Policy		
Next review due by:	July 2024		

DOCUMENT CONTROL

Changes History

Issue No	Date	Amended by	Summary of Changes
1	**28/06/2023**	**Jemma Lynch**	**New Policy**

Authorisation (Responsible Owner)

Name	Role	Approval Date
Jemma Lynch	**Trust Safeguarding Lead**	**19 July 2023**

Approval (Accountable Owner)

Name	Role	Approval Date
Ian Jacobs	**Named Trustee for Safeguarding**	**19 July 2023**

Distribution List – Once authorised (Informed)

Name	
Headteachers Governors Mary Pitchard (for uploading to website)	

Review Period

Date Document Reviewed	By Whom
June 2024	**Trust Safeguarding Lead**

Introduction

Online safety embodies internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

It is essential that children are safeguarded from potentially harmful and inappropriate online material. Our schools will adopt whole school approaches to online safety to protect and educate pupils, students, and staff in their use of technology and establish mechanisms to identify, intervene and escalate concerns as appropriate.

Online safety will be considered when planning the curriculum and teacher training. Staff will reinforce the importance of online safety when communicating with parents. This includes making parents aware of what we ask children to do online (e.g., sites they need to visit or who they'll be interacting with online). A whole school approach to online safety is essential to safeguarding children. It's not the job of one person and it is not just a technical solution. Each school's approach to online safety will be reflected in its child protection procedures.

The key issues around Online Safety affect all schools across Unity Schools Partnership Trust, each school will monitor the impact of the policy using a range of appropriate methods. This may include:

- Logs of reported incidents
- Annual reports to the Academy Council
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of.

    Students / Pupils

    Parents / Carers

The Unity Schools Partnership Online Safety Policy will be reviewed every two years or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. Should serious online safety incidents take place, schools will refer to their Child Protection Procedures and the Trust's Safeguarding Policy.

Scope of the Policy

This policy applies to all members of the Unity Schools Partnership community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of the School / Trusts ICT systems, both in and out of the School / Trust setting.

The Education and Inspections Act 2006 empowers headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place outside of School, but is linked to membership of the Academy.

The 2011 Education Act increased these powers regarding searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy which is unique to each School within the Trust.

Each school across the Trust will deal with such incidents within this policy and associated Behaviour and Anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate behaviour online that takes place outside of school.

Why online activity is important in school

The internet is an essential element for education and social interaction in 21st century life.

- Our schools have a duty to provide children with quality internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and children.
- It is important that children become familiar with Information and Communication Technology (ICT) at an early age, to develop the skills they will need for the remainder of their education and in adult life. ICT enables learners to participate more readily in a rapidly changing world.

- ICT can help engage, motivate, and stimulate children, helping them access new ideas and experiences. Schools use the internet to support lessons in subjects across the curriculum.

- Effective use of the internet enhances pupils' learning. Pupils learn how to use the internet in research, including the skills of knowledge location, retrieval, and evaluation. Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Education and Developing understanding

Students/pupils

We acknowledge that, as well as providing a variety of positive opportunities, the use of technology has become a significant component of many safeguarding issues and can provide a platform that facilitates exploitation of children and young people. The breadth of issues classified within online safety are considerable but can be classified into three areas of risk:

- **Content**: being exposed to illegal, inappropriate, or harmful material
- **Contact**: being subjected to harmful online interaction with other users
- **Conduct**: personal online behaviour that increases the likelihood of, or causes harm, such as the sending of explicit images or online bullying.
- **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Online safety should be in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned E-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited / reviewed.
- Key E-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Students / pupils should be taught in all subjects to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- In lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g., racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable, with clear reasons for the need.

Education – parents / carers

Many parents and carers have only a limited understanding of E-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviors. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Schools across the Trust will therefore seek to provide information and awareness to parents and carers through:

- An E-safety guidance page on each Academy/academy website
- Curriculum activities
- Letters, newsletters, website
- Parents / Carers evenings / sessions
- Reference to relevant web sites / publications e.g.
  www.swgfl.org.uk
  www.saferinternet.org.uk
  www.childnet.com/parents-and-carers
  www.ceop.org
- Identify an online safety lead in each school and publish the details on the school website.

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Online safety issues often relate to issues around safeguarding and staff should ensure they consider this aspect when responding to issues. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff, which will include information on the Trust's filtering and monitoring systems in place. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out periodically.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the Academy online safety Policy and Acceptable Use Agreements.
- This online safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / PD days.
- The safety Coordinator (or other nominated person) will provide advice, guidance and training to individuals as required.

Infrastructure / equipment, filtering, and monitoring

Unity Schools Partnership is responsible for the delivery of high-quality Information and Communication Technology (ICT) service across the Trust, ensuring the continuity of an ICT systems provision that is as safe, secure, compliant and as available as is reasonably acceptable and that policies and procedures approved within this policy are implemented.

- Academy technical systems will be managed in ways that ensure that Trust Academies meet recommended technical requirements and standards.
- A set of regular scheduled tasks are used to ensure safe, secure, compliant and systems.
- Access to physical infrastructure is restricted as much as is practically possible.
- All users will have clearly defined access rights to technical systems and devices, with role-based access rules applied to ensure the highest practical restrictions are in place
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the Trust or internet provider by actively employing the Internet Watch Foundation Policy list. Content lists are regularly updated, and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Unity Schools Partnership uses Smoothwall filtering and monitoring to monitor and record the activity of users on the Academy technical systems and users are made aware of this within the Acceptable Use Policy.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the Academy systems and data. These are tested regularly. The Academy infrastructure and individual workstations are protected by up-to-date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g., trainee teachers, supply teachers, visitors) onto the Academy systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on Academy devices that may be used outside of Academy.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place.

Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees:

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at Academy events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow Academy policies concerning the sharing, distribution, and publication of those images. Those images should only be taken on Academy equipment, if personal equipment is the only device available then staff may use this, copy the material to the Academy network and then remove the material from their device within a reasonable amount of time or ideally as soon as possible.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the Academy into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the Academy website.
- Student's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current Unity Schools Partnership Data Protection & Freedom of Information Policy (GDPR) which all schools within the Trust and their members must adhere to.

Communication

When using communication technologies, Unity Schools Partnership considers the following as good practice:

- The official Academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report to the nominated person the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students / pupils or parents / carers must be professional in tone and content.
- Students / pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the Academy website and only official email addresses should be used to identify members of staff.
- Staff will not use personal e-mail accounts to communicate with anyone in the Academy community (I.e.: Students, Staff, Parents, AC/Governors, Local Authority, Local parish/district councils).

Social Media - Protecting Professional Identity

All Academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Academies and local authorities could be held responsible, indirectly, for the acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race, or disability or who defame a third party may render the Academy or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

Unity Schools Partnership and schools within the Trust, will provide the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff, and the Academy through limiting access to personal information:

- Trust wide policies and procedures; Safeguarding Policy, Staff Code of Conduct, Acceptable use of ICT, GDPR, Online Safety.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Academy staff should ensure that:

  No reference should be made in social media to students / pupils, parents / carers or Academy staff or they do not engage in online discussion on personal matters relating to members of the Academy community.

  Security settings on personal social media profiles are regularly checked to minimise the risk of loss of personal information.

Academy Actions & Sanctions

It is more likely that Unity Schools Partnership and individual schools will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through the normal behaviour / disciplinary policy.

Sanctions include any laid out in Unity Schools Partnership Disciplinary Procedures and other associated Policies.

Unsuitable / inappropriate activities

Some internet activity e.g., accessing child abuse images or distributing racist material is illegal and would obviously be banned from all technical systems. Other activities, e.g., cyber-bullying would be banned and could lead to criminal prosecution. There are, however, a range of activities which may, generally, be legal but would be inappropriate in an educational context, either because of the age of the users or the nature of those activities. The table on the following page offers further guidance on these activities.

Unity Schools Partnership believes that the activities referred to in the following section would be inappropriate in an Academy context and those users, as defined below, should not engage in these activities in an Academy or outside the Academy when using Academy equipment or systems. This Policy restricts usage as follows:

APPENDIX A: Legislation

Academies should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

Computer Misuse Act 1990 This Act

makes it an offence to:

- Erase or amend data or programs without authority.
- Obtain unauthorised access to a computer.
- "Eavesdrop" on a computer.
- Make unauthorised use of computer time or facilities.
- Maliciously corrupt or erase data or programs.
- Deny access to authorised users.

General Data Protection Act 2018

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant, and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they must follow several set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene, or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication, or another article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures.
- Demonstrate standards, which are or ought to be achieved by persons using the system.
- Investigate or detect unauthorised use of the communications system.
- Prevent or detect crime or in the interests of national security.
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible to:
- Ascertain whether the communication is business or personal.
- Protect or support help line staff.
- The Academy reserves the right to monitor its systems and communications in line with its rights under this act.

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene, or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience, or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm, or distress, they:

- This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm, or distress, they:
- Display any writing, sign, or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing, or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality, or ethnic background.

Protection of Children Act 1999

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos, or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the Academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

The Protection of Freedoms Act 2012

Requires Academies to seek permission from a parent / carer to use Biometric systems.

The Academy Information Regulations 2012

Requires Academies to publish certain information on its website.

APPENDIX B: Links to other organisations or documents

The following links may be useful when reviewing or applying the Trust's Online Safety:

Homepage - UK Safer Internet Centre

Childnet — Online safety for young people

Our Helplines - UK Safer Internet Centre

Eliminating Child Sexual Abuse Online – Internet Watch Foundation (iwf.org.uk)

CEOP Safety Centre

CEOP Education (thinkuknow.co.uk)